Nick Clark · Published April 25, 2026 · PDF

Continuous Device Authenticity and Supply-Chain Provenance for Counterfeit-Part Detection in Semiconductor and Defense Procurement

Counterfeit and tampered hardware enters semiconductor and defense supply chains because authenticity is checked once, at an inspection gate, and never again across the part's service life, leaving firmware substitution, recycled die, and broken custody invisible to the buyer who fields the part. This article shows how that gap is closed by the fleet health-monitoring layer of the governed spatial mesh, built on the Health Monitoring inventive step, disclosed in U.S. Provisional Application No. 64/049,409, whose Section 26.8 supply-chain provenance integrity monitor turns device authenticity, firmware integrity, tamper-evident seal status, PUF response consistency, and software bill of materials into continuous credentialed observations rather than one-time gate checks. It composes continuity-based device identity and the dynamic device hash with manufacturing-provenance attestation so degradation, tampering, and spoofing surface as governed observations evaluated against policy.

What This Application Specifies

U.S. Provisional Application No. 64/049,409 discloses health monitoring as a first-class architectural primitive of a governed spatial mesh, and within Chapter 26 it specifies a supply-chain provenance integrity monitoring mechanism (Section 26.8) directed to attesting device and firmware authenticity continuously rather than at a single inspection event. The mechanism comprises a defined set of cooperating evaluators: a device authenticity attestation evaluator producing observations of continuously-valid, expired, revoked, or never-attested authenticity status; a firmware integrity chain monitor tracking firmware updates through the authorized-update-authority chain; a tamper-evident seal monitor producing observations of physical seal status; an authorized-service-provider history recorder producing observations of authorized maintenance, repair, and component-replacement events; a physical-unclonable-function challenge-response monitor producing observations of PUF-response consistency; a manufacturing-provenance chain evaluator verifying the device-to-manufacturer attestation chain; a software bill of materials attestation verifier; and a supply-chain-health lineage recorder.

These evaluators do not operate in isolation. The application grounds device identity in continuity-based device identity rather than enrollment-based public-key infrastructure: each device computes a dynamic device hash that evolves gradually across successive transmissions reflective of its operational state, and a trust-slope validator at each receiver evaluates a newly received hash against the device's recent history. Spoofing, replay, firmware modification, and hardware substitution surface as discontinuities in that slope, detectable regardless of whether an impersonating device possesses a copied credential. The manufacture-time enrollment phase records a manufacture-attestation governed observation binding the device's public credentialing element to a manufacturer identifier, a manufacture-lot identifier, a hardware-revision identifier, and a cryptographic hash of the firmware at manufacture time, signed by a manufacturer authority. The application is explicit that the underlying signature

scheme, attestation primitive, and observation transport are not limiting; the structural commitment is closure of the chain, every authenticity input is credentialed and every authenticity output is itself a credentialed, lineage-recorded observation.

Why It Matters

Hardware assurance in semiconductor and defense procurement has a structural defect: authenticity is a gate, not a state. A part is inspected, sometimes destructively sampled, sometimes electrically tested, at receiving inspection. It passes, enters inventory, and from that moment its authenticity is assumed for the remainder of its service life. Counterfeit-part categories that the gate cannot durably catch, recycled or remarked die sold as new, cloned parts carrying valid-looking markings, parts with substituted or downgraded firmware, parts whose tamper-evident packaging was opened and resealed after the inspection, all defeat a one-time check because the defect either was not present at the gate or is indistinguishable from a genuine part at a single point in time.

The procurement consequence is severe and well documented by the defense acquisition community: counterfeit microelectronics in fielded systems, broken chain of custody between an authorized distributor and a fielded unit, and firmware of unknown provenance running on parts whose hardware is genuine. Zero-trust mandates direct that no device be trusted on the basis of network position or a prior gate check, yet most hardware authenticity programs still resolve to a perimeter assumption: once the part is inside the boundary, it is treated as authentic. The application's contribution matters because it relocates authenticity from a gate event to a continuous observation stream. A device that was genuine at receiving inspection but whose firmware was later substituted, whose seal was later broken, or whose PUF response later drifts out of its enrolled envelope produces an observation that re-enters the assessment, instead of remaining silently inside a trusted boundary.

How It Composes With the Domain

Mapping the Section 26.8 mechanism onto a procurement and sustainment workflow is direct. At wafer fan-out or device personalization, the manufacturing-provenance chain evaluator's enrollment counterpart records the manufacture-attestation observation: the device-specific credentialing element is generated inside a tamper-resistant storage element so the private portion is never exposed, and the public portion is signed together with the manufacturer, lot, hardware-revision, and firmware-hash metadata. A buyer or fielding authority later verifies the device-to-manufacturer attestation chain by retrieving or being presented that observation, so a fictitious device lacking legitimate manufacture-attestation provenance fails verification on its face rather than on a probabilistic test.

Through service life, each evaluator contributes a distinct provenance signal. The firmware integrity chain monitor admits firmware only when it carries credentialed authority signatures validated against the prior firmware-hash history, so an unauthorized firmware load breaks the chain and is recorded with the sandbox-evaluation output rather than applied; a firmware update that fails sandbox evaluation against governance-policy safety properties is not applied. The PUF challenge-response monitor periodically challenges the part and observes response consistency, so a cloned die that cannot reproduce the enrolled physical-unclonable-function response is flagged even when its markings and firmware appear correct. The tamper-evident seal monitor emits a governance-credentialed observation on physical seal status, surfacing a custody break that occurred after the receiving gate. The authorized-service-provider history recorder logs maintenance, repair, and component-replacement events, so an unauthorized component swap appears as an absent or non-credentialed service event. The software bill of materials attestation verifier carries a governance-credentialed SBOM in the device lineage, enabling per-component vulnerability tracking against the parts actually present.

The binding thread is the dynamic device hash. Because identity is continuity-based, hardware substitution and firmware modification produce a detectable discontinuity in the hash sequence independent of the other evaluators, giving a second, identity-layer signal that corroborates a seal break or a failed firmware-chain check. Each evaluator output is routed through authority-filtered emission and recorded by the supply-chain-health lineage recorder, so the buyer receives not a pass or fail flag but a reconstructable provenance record carrying the authority of every contributing observation. The application also composes this supply-chain category with device-operational health and governance-chain integrity into a cross-domain composite, including a device-plus-supply-chain composite wherein operational health and authenticity attestation combine to indicate overall trustworthiness.

What This Enables

The application names the downstream applications its supply-chain provenance observations enable, and each maps to a concrete procurement capability. Zero-trust infrastructure deployment becomes literal at the device layer: every device continuously attests its authenticity rather than relying on network-perimeter security, so a fielded unit's origin is validated on a live observation, not an inventory assumption. Firmware-integrity-gated operation lets a device refuse operation upon detected firmware tampering, converting authenticity from an advisory flag into an operational precondition for high-assurance deployments. Tamper-evident custody for high-security deployments is maintained through continuously-monitored seals, so custody is a monitored state across the part's life rather than a witnessed event at a single handoff. Supply-chain verification lets a buyer validate the authenticity of purchased devices through governance-credentialed attestations, giving acquisition authorities a structural basis for accepting or rejecting a lot.

Because every observation is credentialed and lineage-recorded, the resulting provenance record supports cross-authority interoperability: a manufacturer authority, an authorized distributor, a depot service provider, and a fielding command can each

contribute and consume observations under their own authority position without an out-of-band trust assumption between them. That closure is what a defensible counterfeit-detection and hardware-assurance program needs, and it is supplied as a structural property rather than a documentation exercise.

Boundary Conditions

This article describes what the application discloses; it does not assert detection rates, false-positive rates, or benchmark results, and none should be inferred, the application discloses mechanism and structure, not performance figures. The provenance guarantees are bounded by their physical and cryptographic anchors: PUF challenge-response detection presumes a device with an enrolled physical-unclonable-function, the manufacturing-provenance chain presumes a manufacture-time enrollment was actually performed and recorded, and tamper-evident seal observations are only as strong as the seal hardware reporting them. A device that was never attested produces a never-attested status, which is informative but is not the same as proof of counterfeiting; it marks the part as outside the credentialed population. The mechanism detects discontinuity, substitution, and broken custody as governed observations; it does not by itself adjudicate intent or assign liability, those remain procurement and legal determinations made over the lineage record it produces. Standards and regulatory framing in this article (zero-trust mandates, defense acquisition counterfeit-part concerns, SBOM practice) is external domain context describing where the mechanism applies, not a claim that the application implements any particular standard.

Disclosure Scope

The technical mechanisms described here, the supply-chain provenance integrity monitoring mechanism and its device authenticity attestation evaluator, firmware integrity chain monitor, tamper-evident seal monitor, authorized-service-provider

history recorder, physical-unclonable-function challenge-response monitor, manufacturing-provenance chain evaluator, software bill of materials attestation verifier, and supply-chain-health lineage recorder, together with continuity-based device identity and the dynamic device hash on which they rest, are disclosed in U.S. Provisional Application No. 64/049,409 (Section 26.8 and Chapter 26 generally, with manufacture-time enrollment and firmware-update mechanisms in the device credentialing lifecycle and system-hardening disclosures). The semiconductor and defense procurement framing, counterfeit-part categories, custody and acquisition workflows, zero-trust mandates, and SBOM practices invoked above are external domain and regulatory context provided to show a faithful enabling application of the disclosed mechanism; they are not part of the disclosure and are not claimed here. This article is a dated freedom-to-operate disclosure of how the disclosed health-monitoring layer applies to hardware authenticity and supply-chain provenance and does not constitute legal or procurement advice.

Health & Supply Chain Composite (/health-monitoring)

All 40 steps → (/inventive-steps)

Governance-chain integrity unified with supply-chain provenance. Zero-trust device health.

Provisional application

PRIMARY TECHNICAL DISCLOSURE

- Health Monitoring: Unified Governance and Supply-Chain Composite (/articles/health-monitoring-unified-governance-and-supply-chain-composite)

SECONDARY TECHNICAL

- Governance Chain Integrity Monitoring (/articles/health-monitoring/governance-chain-integrity)
- Trust Slope Anomaly Detection (/articles/health-monitoring/trust-slope-anomaly-detection)
- Revocation Propagation Evaluation (/articles/health-monitoring/revocation-propagation-evaluation)

- PUF Challenge-Response Health Verification (/articles/health-monitoring/puf-challenge-response)
- SBOM Attestation for Software Health (/articles/health-monitoring/sbom-attestation)
- Tamper-Evident Seal Monitoring (/articles/health-monitoring/tamper-evident-seal-monitoring)
- Composite Fleet Health Assessment (/articles/health-monitoring/composite-fleet-health)
- Zero-Trust Device Management (/articles/health-monitoring/zero-trust-device-management)
- Regulatory Compliance Integration (/articles/health-monitoring/regulatory-compliance-integration)

APPLICATIONS · GENERAL

- **Continuous Device Authenticity and Supply-Chain Provenance for Counterfeit-Part Detection in Semiconductor and Defense Procurement (/articles/health-monitoring/device-authenticity-provenance)**
- Defense Fleet Readiness Health Monitoring (/articles/health-monitoring/defense-fleet-readiness)
- Industrial IoT Fleet Health Monitoring for OT Security and Compliance (/articles/health-monitoring/industrial-iot-fleet-monitoring)
- Medical Device Fleet Health Monitoring (/articles/health-monitoring/medical-device-fleet-monitoring)
- Automotive Cybersecurity Compliance Under UN ECE R155 and R156: A Fleet Health Monitoring Substrate for CSMS Evidence (/articles/health-monitoring/automotive-cybersecurity-uneces)
- Continuous Device-Integrity Evidence for CISA-Regulated Critical Infrastructure Fleets (/articles/health-monitoring/critical-infrastructure-fleet-cisa)
- Medical Device Cybersecurity Fleet Management Under FDA 524B (/articles/health-monitoring/medical-device-cybersecurity)
- AAMI TIR57 Compliance for Connected Medical Devices: An Attested Health-Monitoring Substrate (/articles/health-monitoring/aami-tir57-medical-cyber)
- CMMC 2.0 Defense Contractor Cybersecurity Compliance: Device Integrity Evidence for C3PAO Assessment (/articles/health-monitoring/cmmc-2-defense-cyber)
- DO-326A Airworthiness Security Compliance for Aircraft Fleet Cybersecurity (/articles/health-monitoring/do-326a-aviation-cyber)
- IEC 62443 Compliance for Industrial Control Systems: Architectural Device Evidence at Fleet Scale (/articles/health-monitoring/iec-62443-industrial-cyber)
- ISO 13485 Compliance for Connected Medical Device Fleets: Continuous Attestation for Post-Market Surveillance (/articles/health-monitoring/iso-13485-medical-qms)
- Continuous Device Attestation Evidence for NIST CSF 2.0 Compliance Across Device Fleets (/articles/health-monitoring/nist-csf-2-0)

APPLICATIONS · SPECIFIC

- CrowdStrike Falcon Lacks Architectural Composite Fleet Health (/articles/health-monitoring/crowdstrike-falcon-fleet)
- Medtronic CareLink Lacks Architectural Medical-Device Fleet Substrate (/articles/health-monitoring/medtronic-carelink)
- Microsoft Defender Lacks Cross-Fleet Composite Substrate (/articles/health-monitoring/microsoft-defender-fleet)
- Armis Asset Management Lacks Architectural Fleet-Health Substrate (/articles/health-monitoring/armis-iot-asset)
- Claroty xDome OT Security Lacks Cross-Vendor Fleet-Health (/articles/health-monitoring/claroty-ot)
- Dragos Industrial Cybersecurity Lacks Cross-Vendor Fleet-Health (/articles/health-monitoring/dragos-industrial)
- Nozomi Networks Lacks Cross-Vendor Fleet-Health Substrate (/articles/health-monitoring/nozomi-networks)
- Tenable OT Security Lacks Cross-Vendor Fleet-Health Substrate (/articles/health-monitoring/tenable-iot-ot)
- AVEVA (Schneider) Industrial Software (/articles/health-monitoring/schneider-aveva)

Health & Supply Chain Composite overview → (/health-monitoring)